ОТСЛЕЖИВАНИЕ МАРШРУТА ПЕРЕМЕЩЕНИЙ ФАЙЛА МЕЖДУ КОМПЬЮТЕРАМИ ЛОКАЛЬНОЙ СЕТИ

Доронин А. К.

УО «Гродненский государственный университет им. Я. Купалы», Гродно,
e-mail: mail@grsu.by

Задача отследить маршрут перемещений файла между компьютерами в локальной сети часто возникает при работе с документами. К примеру, необходимо узнать, у кого в данный момент находится файл, который должен передаваться по очереди. Без использования специальных дорогих программ, решить данную задачу весьма сложно. К тому же, указанные программы (к примеру, InfoWatch Traffic Monitor) осуществляют глобальный мониторинг траффика и достаточно сложны в освоении. В данной работе предложен метод, позволяющий добиться решения без использования значительных затрат с помощью альтернативных потоков данных.

Альтернативные потоки данных (далее - ADS) — это метаданные, связанные с объектом файловой системы NTFS. В файловой системе NTFS файл, кроме основных данных, может также быть связан с одним или несколькими дополнительными потоками данных. При этом дополнительный поток может быть произвольного размера, в том числе может превышать размер основного файла. Альтернативные потоки данных игнорируются большинством программ, включая Windows Explorer. Windows Explorer не подсчитывает размер и не отображает список альтернативных потоков. Следовательно, возможно хранить историю изменений файла скрытно от пользователя.

Для применения данного метода необходимо разработать программы (модули) мониторинга и управления. Программа управления должна иметь функцию задания маски имен отслеживаемых файлов, а также функцию графического отображения маршрута перемещений данных файлов. Модуль мониторинга должен устанавливаться на конечных ПК локальной сети, помечать ADS необходимые файлы и отслеживать любые изменения с ними, записывать информацию об изменениях в ADS файла.

Проблемой остается наличие у пользователя многочисленных возможностей передачи файлов. Поэтому необходимо учесть основные способы копирования, которые наиболее часто использует пользователь, и учесть это в программной реализации.

В данной работе исследована задача отслеживания маршрута перемещений файла в локальной сети. Были рассмотрены программы, реализующие данную функцию, их основные недостатки, а также предложен новый подход к решению данной задачи на основе альтернативных потоков данных в NTFS. Предложена схема реализации программной части метода и рассмотрены сопутствующие проблемы.

Литература